

Rec'd ~~PCT/EP~~ 25 JAN 2005

REC'D 10 OCT 2003

WIPO

PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)



**Prioritätsbescheinigung über die Einreichung
einer Patentanmeldung**

Aktenzeichen: 102 34 158.3

Anmeldetag: 26. Juli 2002

Anmelder/Inhaber: Giesecke & Devrient GmbH, München/DE

Bezeichnung: Einrichten eines Dateisystems in einem Datenträger

IPC: G 06 F 12/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 19. August 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hintermeier

Einrichten eines Dateisystems in einem Datenträger

Die Erfindung betrifft allgemein das technische Gebiet, ein Dateisystem in einem tragbaren Datenträger, wie z.B. einer Chipkarte oder einem Chip-
5 modul, einzurichten.

Bevor ein Datenträger einsatzbereit ist, muß in ihm ein Dateisystem eingerichtet werden. Dies geschieht typischerweise im Zuge der Initialisierung des Datenträgers, also beim Einspielen von Daten und/oder Programmen,
10 die für eine größere Anzahl von Datenträgern identisch sind. Mit diesem Einspielen von Daten werden auch die Strukturen und Attribute (Dateibaum, Leserechte usw.) des Dateisystems ganz oder teilweise festgelegt. Das Dateisystem kann auch bei anderen Fertigungsschritten eingerichtet werden, z.B. bei der Personalisierung, also dem Einspielen von
15 Daten, die für den Datenträger bzw. dessen späteren Benutzer individuell sind.

In der Norm ISO 7816 wird beschrieben, wie ein normgemäßes Dateisystem in Chipkarten angelegt werden kann. Insbesondere behandelt ISO 7816-9
20 den Befehl CREATE FILE, mit dem sich die einzelnen Dateien des Dateisystems und die dazugehörigen Dateiattribute sukzessive anlegen lassen. Die Parameter des Befehls CREATE FILE sind so gestaltet, daß Bitfolgen aus den an die Chipkarte übermittelten Daten unmittelbar, also ohne weitere Umsetzung, in einen Speicher der Chipkarte geschrieben werden.

25 Das genaue Format der zur Dateisystem-Initialisierung in die Chipkarte übertragenen Daten ist meist proprietär und kann von dem jeweiligen Betriebssystem der Karte abhängen. Dies gilt insbesondere dann, wenn die Karte gegenüber der genannten Norm Änderungen oder Weiter-
30 entwicklungen aufweist, aber auch in anderen Fällen, weil die Norm einen gewissen Interpretationsspielraum zuläßt. Überdies kommen zunehmend

Chipkarten zum Einsatz, deren Dateisystem nicht gemäß ISO 7816 initialisiert werden kann oder bei denen dies zumindest nicht üblich ist, wie z.B. die Java Card™.

- 5 Wegen der starken Maschinenorientierung der üblichen Formate sind zum Erstellen und Bearbeiten der Initialisierungsdaten spezielle Hilfsprogramme erforderlich, die ebenfalls an die jeweils verwendete Chipkarte und deren Betriebssystem angepaßt sein müssen. Ein derartiges Hilfsprogramm, das für das Chipkarten-Betriebssystem STARCOS® der Anmelderin zugeschnitten
- 10 ist, wird gegenwärtig unter der Bezeichnung STARMAG® vertrieben. Auch hier besteht das Problem, daß einerseits das STARMAG®-Programm nicht oder nur eingeschränkt für Chipkarten mit anderen Betriebssystemen verwendbar ist, und daß andererseits möglicherweise nützliche Funktionen anderer Programme nicht für STARCOS®-Chipkarten zur Verfügung stehen.

15

- Die bislang genannten Probleme bestehen nicht nur im Hinblick auf das Format der in die Chipkarte zu übertragenden Daten, sondern ebenso im Hinblick auf das Datenformat, in dem die benötigten Informationen über das anzulegende Dateisystem einer Initialisierungs- und/oder Personalisie-
- 20 rungsvorrichtung für Chipkarten übermittelt werden. Auch hier werden proprietäre Formate eingesetzt, die überdies von den jeweils zu bearbeitenden Chipkarten abhängen und spezielle Hilfsprogramme erfordern.

- Die Erfindung hat die Aufgabe, die genannten Probleme ganz oder zum Teil
- 25 zu lösen. Insbesondere soll durch die Erfindung eine Technik zum Einrichten eines Dateisystems in einem Datenträger bereitgestellt werden, die die bisherige starke Abhängigkeit zwischen dem verwendeten Dateiformat und Betriebssystem-Interna des Datenträgers verringert. In bevorzugten Ausgestaltungen sollen marktübliche Hilfsprogramme und Werkzeuge universell,

also im Zusammenhang mit Dateisystem-Einrichtungsdaten für die unterschiedlichsten Datenträger, einsetzbar sein.

5 Erfindungsgemäß wird diese Aufgabe ganz oder zum Teil gelöst durch ein Verfahren mit den Merkmalen von Anspruch 1, einen tragbaren Datenträger gemäß Anspruch 8, eine Initialisierungs- und/oder Personalisierungs-
vorrichtung nach Anspruch 9 und einen computerlesbaren Datenträger gemäß Anspruch 10. Die abhängigen Ansprüche definieren bevorzugte Ausgestaltungen der Erfindung.

10

Die Erfindung geht von der Kombination zweier Grundideen aus. Erstens werden Spezifikationsdaten verwendet, die das im Datenträger einzurichtende Dateisystem zumindest zum Teil auf semantischer Ebene beschreiben. Zweitens werden diese Spezifikationsdaten von einem Prozessorkern des
15 Datenträgers interpretiert. In diesem Zusammenhang soll unter einer Interpretation stets eine gewisse Verarbeitung und Umwandlung der Daten verstanden werden. Ein unverändertes Einschreiben von empfangenen Bitfolgen in einen Speicher des Datenträgers ist im allgemeinen keine Interpretation in diesem Sinne.

20

Durch die Erfindung wird eine erhebliche Abstraktion von Einzelheiten des Datenträger-Betriebssystems erreicht. Dadurch, daß die Interpretation der Spezifikationsdaten durch den Datenträger selbst vorgenommen wird, brauchen externe Systeme keine Interna des Betriebssystems zu kennen,
25 sondern können vielmehr gleichermaßen im Zusammenhang mit unterschiedlichen Typen von Datenträgern verwendet werden. Es entfällt also die Notwendigkeit, Datenstrukturen in dem für die Ablage benötigten speziellen Format bereitzustellen. Die so erzielte technische Vereinheitlichung bewirkt erhebliche Einsparungen im Hinblick auf Geräte, Software und Ausbildung

von Mitarbeitern. Überdies steigt durch die Abkapselung interner Datenstrukturen die Sicherheit des Gesamtsystems gegen ungewollte Fehlkonfiguration oder absichtliche Manipulation.

- 5 Die Aufzählungsreihenfolge der Schritte in den Verfahrensansprüchen soll nicht als Einschränkung des Schutzbereichs verstanden werden. Es sind vielmehr Ausgestaltungen der Erfindung vorgesehen, bei denen diese Verfahrensschritte in anderer Reihenfolge oder ganz oder teilweise parallel oder ganz oder teilweise ineinander verzahnt (*interleaved*) ausgeführt werden.
- 10 Insbesondere werden in bevorzugten Ausgestaltungen die Spezifikationsdaten Stück für Stück oder in einem kontinuierlichen Strom in den Datenträger eingelesen und jeweils abschnittsweise interpretiert, wobei die bei der Interpretation ermittelten Teile des Dateisystems jeweils sofort in den Speicher des Datenträgers eingeschrieben werden.
- 15 In bevorzugten Ausgestaltungen der Erfindung beschreiben die Spezifikationsdaten die Dateien des Dateisystems und die zugehörigen Dateiattribute. Die Dateiattribute können Sicherheitseinstellungen, wie z.B. Lese-, Schreib- und Ausführungsrechte, und/oder Protokolleinstellungen, wie z.B. eine
- 20 Übertragung per *Secure Messaging* oder *Secure Sockets Layer* (SSL), definieren. Ferner können die Spezifikationsdaten Relationen zwischen Dateien des Dateisystems angeben, z.B. die Relation, daß zwei Dateien ein Schlüsselpaar bilden, die Relation, daß eine Datei ein Zertifikat für einen Schlüssel darstellt, oder die Relation Datei/Eigentümer. Durch diese möglichen
- 25 Inhalte stellen die Spezifikationsdaten in bevorzugten Ausführungsformen ein mächtiges Beschreibungsmittel für das Dateisystem dar.

Die Spezifikationsdaten weisen bevorzugt ein textuelles und/oder portables und/oder interoperables Datenformat auf. Durch diese Maßnahmen lassen

sich Werkzeuge und Hilfsprogramme gleichermaßen für unterschiedliche Datenträger einsetzen. In manchen Ausgestaltungen werden weit verbreitete Standard-Datenformate eingesetzt, wie z.B. XML (*extensible markup language*), oder Formate entsprechend den Codierregeln DER (*distinguished encoding rules*) oder BER (*basic encoding rules*) oder PER (*packed encoding rules*), die für
5 Datenstrukturen vorgesehen sind, welche in ASN.1 (*abstract syntax notation no. 1*) definiert sind.

10 Für standardisierte Datenformate wie die oben genannten steht eine Vielzahl von universell verwendbaren Werkzeugen zur Verfügung. Beispielsweise können Spezifikationsdaten im XML-Format mittels üblicher Web-Browser visualisiert werden. Auch sind derartige Formate vielen Entwicklungs-
ingenieuren bereits bekannt, so daß keine aufwendigen Schulungen erforderlich sind. Die Spezifikationsdaten können in einer einzigen Datei
15 zusammengefaßt sein oder in Form von mehreren Dateien vorliegen.

Die Spezifikationsdaten werden der Initialisierungs- oder Personalisierungs-
vorrichtung vorzugsweise bereits in demjenigen Format vorgelegt, in dem
sie dann auch an den Datenträger übertragen werden. Eine solche Ausgestal-
20 tung hat den Vorteil, daß die Initialisierungs- oder Personalisierungsvorrich-
tung ohne oder mit nur geringem Einstellungsaufwand für unterschiedliche
Datenträger einsetzbar ist. Insbesondere dann, wenn die Initialisierung oder
Personalisierung von externen Dienstleistern vorgenommen wird, werden
die Spezifikationsdaten vorzugsweise durch kryptographische Mittel, wie
25 z.B. Verschlüsselung und/oder Signatur, gegen Manipulation und/oder
Ausspähung geschützt. Die Entschlüsselung bzw. Prüfung der Signatur
kann durch den Datenträger selbst vorgenommen werden, so daß außerhalb
des Datenträgers keine Angriffsmöglichkeiten bestehen.

Der tragbare Datenträger, die Initialisierungs- und/oder Personalisierungsvorrichtung und der computerlesbare Datenträger weisen in bevorzugten Weiterbildungen Merkmale auf, die den oben erwähnten und/oder den in den abhängigen Verfahrensansprüchen genannten Merkmalen entsprechen.

- 5 Der erfindungsgemäße computerlesbare Datenträger, der die Spezifikationsdaten beinhaltet, braucht nicht notwendigerweise materieller Natur zu sein. Auch ein zur Datenübertragung geeignet modulierte elektrisches oder elektromagnetisches Signal kann ein computerlesbarer Datenträger in diesem Sinne sein.

10

Weitere Merkmale, Aufgaben und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung mehrerer Ausführungsbeispiele und Ausführungsalternativen. Es wird auf die schematischen Zeichnungen verwiesen, in denen zeigen:

15

Fig. 1 ein Blockdiagramm von Komponenten, die an einem Ausführungsbeispiel des erfindungsgemäßen Verfahrens beteiligt sind, und

20

Fig. 2 eine beispielhafte Darstellung von Spezifikationsdaten, die als XML-Datei vorliegen.

25

In Fig. 1 ist ein tragbarer Datenträger 10 gezeigt, der beispielsweise als Chipkarte oder Chipmodul ausgebildet ist. In an sich bekannter Weise weist der Datenträger 10 einen Halbleiterchip auf, auf dem ein Prozessorkern 12, ein Speicher 14 und eine Schnittstelle 16 zur drahtgebundenen oder drahtlosen Kommunikation ausgebildet sind. Der Speicher 14 weist mehrere in unterschiedlichen Schaltungstechniken ausgebildete Bereiche auf, nämlich im vorliegenden Ausführungsbeispiel einen ROM-Bereich 18 mit maskenprogrammiertem Festwertspeicher, einen RAM-Bereich 20 mit flüchtigem

Schreib-/Lese-Speicher und einen Bereich 22 mit nicht-flüchtigem, wiederbeschreibbarem Speicher, z.B. EEPROM, Flash-Speicher usw.

- Der ROM-Bereich 18 des Speichers 14 enthält das Betriebssystem und die von diesem Betriebssystem ausgeführten Programme des Datenträgers 10. Als Teil des Betriebssystems ist insbesondere ein Interpreter 24 vorgesehen, dessen Funktion später noch genauer erläutert werden wird. Ein Dateisystem 26 soll im EEPROM-Bereich 22 angelegt werden. In Fig. 1 ist zur Veranschaulichung ein Ausschnitt des Dateisystems 26 gezeigt, das der Norm ISO 7816 entspricht und eine Wurzel MF (*master file*) sowie mehrere Hierarchieebenen von Verzeichnissen DF (*dedicated file*) und Einzeldateien EF (*elementary file*) aufweist. In Ausführungsvarianten wird das Dateisystem 26 gemäß anderen Konventionen oder Normen angelegt.
- Der Datenträger 10 ist an eine Vorrichtung 28 angeschlossen, die zur Initialisierung und/oder Personalisierung des Datenträgers 10 dient. Die Vorrichtung 28 kann beispielsweise als an sich bekanntes Initialisierungssystem oder als Personalisierungssystem oder – in besonders einfachen Ausgestaltungen – als Computer mit einer geeigneten Schnittstelle zur Ankopplung an den Datenträger 10 ausgestaltet sein. Die Vorrichtung 28 liest Spezifikationsdaten SD von einem computerlesbaren Datenträger 30 aus, der z.B. als Diskette oder CD-ROM ausgebildet sein kann. Die Spezifikationsdaten SD werden von der Vorrichtung 28 im vorliegenden Ausführungsbeispiel als Kommando-APDU (*application protocol data unit*) 32 an den Datenträger 10 übertragen.

Die Spezifikationsdaten SD enthalten eine Beschreibung des im Datenträger 10 anzulegenden Dateisystems 26 auf semantischer Ebene. Dies heißt im vorliegenden Ausführungsbeispiel, daß die Spezifikationsdaten SD die Struktur

des Dateisystems 26 sowie Dateiattribute und Beziehungen zwischen Dateien in einer abstrakten Form angeben, die von der Struktur der Bitfolgen der im Speicher 14 anzulegenden Verwaltungsdaten unabhängig ist. Die Spezifikationsdaten SD können als eine einzige Datei vorliegen oder auf
5 mehrere Dateien verteilt sein. Beispielsweise kann eine erste Spezifikationsdatei verwendet werden, um Benutzerinformationen anzulegen, eine zweite Spezifikationsdatei, um die Struktur des Dateisystems 26 zu erzeugen, eine Dritte, um Benutzer in Gruppen zusammenzufassen, und so weiter. In Ausgestaltungen, die mehrere
10 Spezifikationsdateien verwenden, werden bevorzugt entsprechend viele Kommando-APDUs 32 an den Datenträger 10 gesendet.

Ein Beispiel für Spezifikationsdaten SD, die in einem portablen und interoperablen XML-Format vorliegen, ist in Fig. 2 dargestellt. Die Dateitypen
15 MF, DF und EF des Dateisystems 26 werden hier durch entsprechende XML-Tags <MF ...>, <DF ...> und <EF ...> repräsentiert, und die Verschachtelung dieser Tags in den Spezifikationsdaten SD gibt die Baumstruktur des zu erzeugenden Dateisystems 26 an. Dateiattribute im Dateisystem 26 werden in den Spezifikationsdaten SD durch entsprechende XML-Attribute dargestellt.
20 So finden sich beispielsweise die grundlegenden Namensattribute FID (*file identifier*) und AID (*application identifier*) als XML-Attribute der Tags <DF ...> und <EF ...> wieder. Weitere XML-Attribute geben die Dateiart (*type*) und die maximale Dateigröße (*maxsize*) an.

25 In den Spezifikationsdaten SD werden im vorliegenden Ausführungsbeispiel ferner Sicherheitseinstellungen der einzelnen Dateien definiert, z.B. in Fig. 2 durch die XML-Attribute *access*, *owner*, *group* und *mode*. Schließlich werden auch Verknüpfungen zwischen Dateien definiert, z.B. in Fig. 2 durch das XML-Attribut *LinkTo*. In den Spezifikationsdaten SD können weitere Anga-

ben zu der anzulegenden Dateistruktur 26 oder zu anderen Initialisierungs- oder Personalisierungswerten für den Datenträger 10 enthalten sein. Einige Beispiele für derartige Angaben sind in Fig. 2 gezeigt.

- 5 Zur Initialisierung oder Personalisierung des Datenträgers 10 in dem System von Fig. 1 werden zunächst die Spezifikationsdaten SD erstellt. Wenn es sich um ein textuelles Datenformat handelt, kann dazu ein gewöhnlicher Text-
editor dienen. Für andere strukturierte Datenformate kann ein geeignetes
Werkzeug, beispielsweise ein XML-Generator, eingesetzt werden. Zur
10 Visualisierung kann ein üblicher Web-Browser dienen.

- Die erstellten Spezifikationsdaten SD werden auf dem computerlesbaren
Datenträger 30 gespeichert und von dort in die Initialisierungs- und/oder
Personalisierungsvorrichtung 28 eingelesen. Im vorliegenden Ausführungs-
15 beispiel führt die Vorrichtung 28 keine inhaltliche Bearbeitung der Spezifika-
tionsdaten SD durch, sondern "verpackt" diese Daten lediglich in einer geeig-
neten Kommando-APDU 32, die zum tragbaren Datenträger 10 übertragen
wird.

- 20 Der Prozessorkern 12 des Datenträgers 10 empfängt die Kommando-APDU
32 über die Schnittstelle 16 und extrahiert die darin enthaltenen Spezifika-
tionsdaten SD. Gesteuert vom Interpreter 24 interpretiert der Prozessorkern
12 die Spezifikationsdaten SD und legt das darin beschriebene Dateisystem
26 Stück für Stück im EEPROM-Bereich 22 des Speichers 14 an. Hierbei
25 werden die einzelnen Dateien erzeugt und die Dateiattribute einschließlich
der Sicherheitseinstellungen entsprechend den interpretierten Spezifika-
tionsdaten SD gesetzt. Ferner werden Relationen zwischen Dateien definiert
und sonstige Einstellungen gemäß den Spezifikationsdaten SD vorgenom-
men.

Bei der Interpretation durch den Prozessorkern 12 werden im vorliegenden Ausführungsbeispiel unbekannte Elemente der Spezifikationsdaten SD, z.B. unbekannte XML-Tags, einfach ignoriert. Dadurch sind Ergänzungen oder
5 Erweiterungen des Formats der Spezifikationsdaten SD möglich, wobei auch Spezifikationsdaten SD im erweiterten Format von Datenträgern 10, die dieses Format nicht beherrschen, nach wie vor interpretiert werden können. Die strukturelle Identität der bekannten Elemente des Spezifikationsdaten-Formats geht also nicht verloren.

10

Die Spezifikationsdaten SD können auf dem computerlesbaren Datenträger 30 und/oder bei der Übertragung zum tragbaren Datenträger 10 in verschlüsselter und/oder signierter Form vorliegen. Die Entschlüsselung bzw. Signaturkontrolle findet dann erst im tragbaren Datenträger 10 statt. Da im
15 vorliegenden Ausführungsbeispiel die Vorrichtung 28 keine inhaltliche Veränderung der Spezifikationsdaten SD vornimmt, braucht hier keine Entschlüsselung zu erfolgen. Für den Initialisierungs- bzw. Personalisierungsvorgang ist somit keine gesicherte Umgebung erforderlich.

Patentansprüche

1. Verfahren zum Einrichten eines Dateisystems (26) in einem tragbaren Datenträger (10), der einen Prozessorkern (12) und mindestens einen Speicher (14) aufweist, mit den Schritten:
 - Einlesen von Spezifikationsdaten (SD), die das Dateisystem (26) zumindest zum Teil auf semantischer Ebene beschreiben,
 - Interpretieren der eingelesenen Spezifikationsdaten (SD) durch den Prozessorkern (12), und
 - Einrichten des Dateisystems (26) gemäß den interpretierten Spezifikationsdaten (SD) in dem mindestens einen Speicher (14) des Datenträgers (10).
2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Spezifikationsdaten (SD) die Dateistruktur des Dateisystems (26) einschließlich Dateiattributen beschreiben.
3. Verfahren nach Anspruch 2, dadurch **gekennzeichnet**, daß die Dateiattribute Sicherheitseinstellungen und/oder Protokolleinstellungen und/oder Benutzer/Gruppenzuordnungen angeben.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß die Spezifikationsdaten (SD) Relationen zwischen Dateien des Dateisystems angeben.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, daß die Spezifikationsdaten (SD) in einem textuellen und/oder portablen und/oder interoperablen Format vorliegen.

- 5
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, daß die Spezifikationsdaten (SD) in XML und/oder in einer Codierung gemäß Codierregeln für ASN.1-definierte Datenstrukturen vorliegen.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch **gekennzeichnet**, daß die Spezifikationsdaten (SD) kryptographisch gegen Manipulation und/oder Ausspähung geschützt sind.
- 10
8. Tragbarer Datenträger (10), insbesondere Chipkarte oder Chipmodul, mit einem Prozessorkern (12) und mindestens einem Speicher (14), der dazu eingerichtet ist, ein Verfahren nach einem der Ansprüche 1 bis 7 auszuführen.
- 15
9. Vorrichtung (28) zur Initialisierung und/oder Personalisierung eines tragbaren Datenträgers (10) nach Anspruch 8, die dazu eingerichtet ist, Spezifikationsdaten (SD), die ein in dem tragbaren Datenträger (10) einzurichtendes Dateisystem (26) zumindest zum Teil auf semantischer Ebene beschreiben, an den tragbaren Datenträger (10) zu übertragen.
- 20
10. Computerlesbarer Datenträger (30) mit Spezifikationsdaten (SD), die dazu eingerichtet sind, in einen tragbaren Datenträger (10) eingelesen und dort nach einem Verfahren nach einem der Ansprüche 1 bis 7 interpretiert zu werden.
- 25

Zusammenfassung

Einrichten eines Dateisystems in einem Datenträger

- 5 Ein Verfahren zum Einrichten eines Dateisystems (26) in einem tragbaren Datenträger (10) weist die Schritte auf, Spezifikationsdaten (SD), die das Dateisystem (26) zumindest zum Teil auf semantischer Ebene beschreiben, einzulesen, die eingelesenen Spezifikationsdaten (SD) durch einen Prozessor (12) des Datenträgers (10) zu interpretieren, und das Dateisystem (26) gemäß den interpretierten Spezifikationsdaten (SD) in einem Speicher (14) des Datenträgers (10) einzurichten. Ein computerlesbarer Datenträger (30) und eine Vorrichtung (28) zur Initialisierung und/oder Personalisierung eines tragbaren Datenträgers (10) sind dazu eingerichtet, Spezifikationsdaten (SD) zu speichern bzw. in einen erfindungsgemäßen tragbaren Datenträger (10) zu übertragen. Die Erfindung stellt eine Technik zum Einrichten eines Dateisystems (26) in einem Datenträger (10) bereit, die die bisherige starke Abhängigkeit zwischen dem verwendeten Dateiformat und Betriebssystem-Internen des Datenträgers (10) verringert.

20 (Fig. 1)

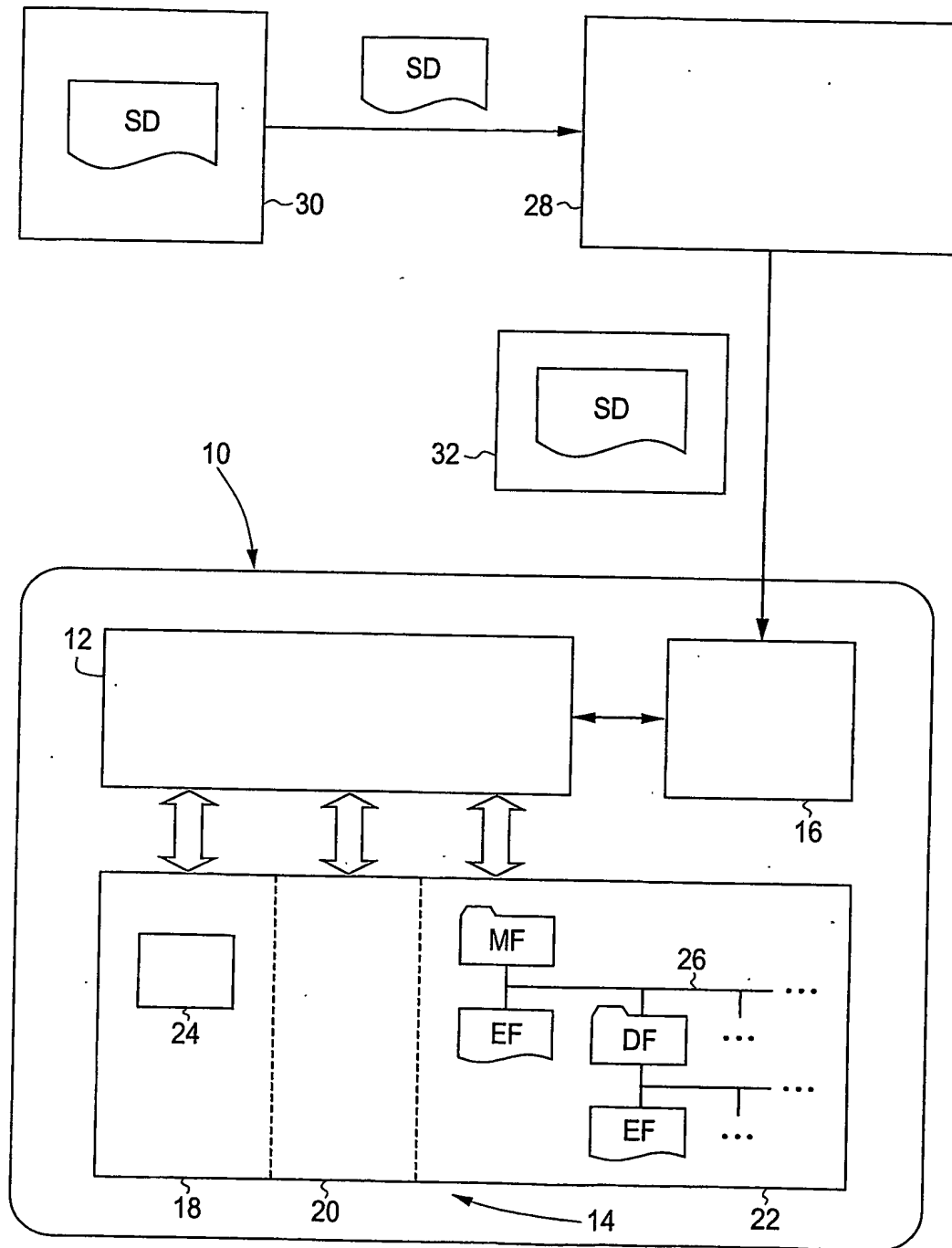


Fig. 1

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE filesystem SYSTEM "ISO7816.dtd">
<filesystem>
  <Group GroupID="perso" />
  <Group GroupID="users" />
  <Group GroupID="signers" />
  <Group GroupID="webusers" />
  <Personality UserID="Personalisation" PIN="123456"
    Groups="perso"
    Options="RemoveAfterLogout" />
  <Personality UserID="Notar" PIN="11111"
    Groups="users,signers,webusers"
    Options="LogoutAfterSign" />
  <Personality UserID="Public" PIN="123456" />
  <MF>
    <DF AID="#D276000005100C" FID="DF01" access="rw">
      <EF FID="C000" owner="Notar" group="signers"
        mode="rw-r--r--" LinkTo="DF01.ISF.RSA01"
        type="transparent" maxsize="2048" />
      <EF FID="C008" owner="Notar" group="webusers"
        mode="rw-r--r--" LinkTo="DF01.ISF.RSA02"
        type="transparent" maxsize="2048" />
      <ISF>
        <Key KID="01" Type="RSA" Usage="Signhash"
          owner="Notar" group="signers"
          mode="rw-----" />
        <Key KID="02" Type="RSA" Usage="SSL"
          owner="Notar" group="webusers"
          mode="rw-r-----" />
      </ISF>
    </DF>
  </MF>
  <EXE>
    <EXF EID="genrsa" owner="Personalisation"
      group="users" mode="rw---x---" />
    <EXF EID="signhash" owner="Personalisation"
      group="signers" mode="rw---x---" />
    <EXF EID="sslauth" owner="Personalisation"
      group="webusers" mode="rw---x---" />
  </EXE>
</filesystem>

```

Fig. 2

SD

